CP-DevSecOps

CP-DevSecOps PROGRAM HIGHLIGHTS

- CP-DevSecOps focuses on the most challenging areas for security testing of web applications in the DevOps scenario using tools like Arachni, Gauntlt, Gauntlt-Docker, Metasploit, ZAP & Burp.
- Understand concepts like Rugged Manifesto, OWASP top 10 and WebPenetration Testing
- Using tools in BurpSuite to launch a Brute-Forcing attack, XSS attack and a SQLi attack
- Using Gauntlt to launch and automate XSS attack, SQLi attack, fuzzer and network tests
- Using Arachni for implementing Crawl Coverage and Vulnerability Detection
- Using Zed Attack Proxy and integrating with CI/CD tool
- Implementing the entire security testing using Jenkins/Docker

Practically experience and learn DevSecOps

Understand, Implement and Automate Security tests in DevOps

CP-DevSecOps is the surest way for you to practically experience contiuous security testing or DevSecOps using the most in demand open source tools like Burp, Gauntlt, Gauntlt-Docker, Metasploit and ZAP

Tool Coverage

BURPSUITE arachni web application security scanner framework

GAUNTLT BE MEAN TO YOUR CODE AND LIKE IT RAPID7 etasploit

+91-8433919049
info@devopsppalliance.org
http://cpdevsecops.devopsppalliance.org